NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 2810.1A
Effective Date: May 16, 2006
Expiration Date: May 16, 2011

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: Security of Information Technology

Responsible Office: Office of the Chief Information Officer

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | Chapter12 | Chapter13 | Chapter14 | Chapter15 | Chapter16 | Chapter17 | Chapter18 | Chapter19 | Chapter20 | Chapter21 | AppendixA | AppendixB | ALL |

Chapter 16 Network and Systems Monitoring

16.1 Monitoring of Electronic Data on NASA Computer Networks

16.1.1 Monitoring of computer network traffic refers to the capture of electronic data while in transit or in storage and the subsequent inspection of protocols, ports, and contents of data packets, either in its raw or reconstituted form.

16.1.2 Purpose of Monitoring

16.1.2.1 NASA will continuously monitor electronic communications to ensure the productivity of its workforce, to gauge the performance and availability of its networks and services, and to secure its data and information systems from hostile intrusions, misuse, and other threats.

16.1.2.2 The monitoring (encrypted or unencrypted) of inbound or outbound traffic on any NASA network will be based on risk management principles, with a higher concentration on those assets deemed most critical to NASA.

16.1.2.3 NASA's IT resources are the property of the U.S. Government. Therefore NASA maintains the right to monitor all aspects of computer usage at any time. NASA policy states clearly that employees, including civil servants, support service contractors, grantees, and students do not have any expectation of privacy in any message, file, image or data created, sent, retrieved, or received by use of Government resources.

16.1.3 Routine Monitoring Requirements

16.1.3.1 IT security staff shall conduct continuous monitoring of NASA networks at multiple locations to ensure availability of networks and services and to detect and protect the network against hostile intrusions, misuse, and other threats.

16.1.3.2 Monitoring can include ports, IP addresses, protocols, and content. Monitoring shall be performed either by automated means, such as intrusion detection systems and flow-based content monitors, or by manual inspection of the contents of captured network data or log data. A diverse and dynamic range of computer tools are used and tested to perform monitoring activities.

16.1.3.3 Types of monitoring for hostile computer activities include the following:

a. Traffic and trend analysis.

b. Monitoring for illegal software and malicious code.

c. Enforcement of IT and IT security policies.

d. Monitoring for unauthorized network devices, services, ports, or protocols.

16.1.3.4 Routine monitoring of NASA electronic communications may be performed by:

a. Center ITSMs.

b. Center IT security personnel designated by the Center CIO.

c. NASA IT security personnel designated by the SAISO.

d. IT administrators (e.g., computer systems administrators and network administrators) within the narrow scope of normal IT administrative duties on networks under their purview.

16.1.3.5 Routine monitoring to ensure workforce productivity, the availability of networks and services, and the security of data and information systems is authorized under the Electronic Communications Privacy Act.

16.1.3.6 If suspicious traffic, criminal or non-criminal, is discovered during the course of routine monitoring, incident response and/or misuse policies shall be followed. Subsequently, if targeted monitoring is required, a request shall be submitted through the appropriate management chain.

16.1.4 Targeted Monitoring Requirements

16.1.4.1 Specific and prolonged monitoring of NASA electronic communications by NASA IT or IT security personnel can be triggered by a discovery of anomalous traffic or behavior during routine monitoring, by a formal request from a manager, or by a formal request from a law enforcement organization.

16.1.4.2 Targeted monitoring may be initiated for the following reasons:

a. A higher than expected volume of network traffic is detected on an individual's system.

b. Hostile, threatening, suspicious, unauthorized, or unusual network traffic is detected.

c. Connections to known hostile or suspicious sites are identified.

d. Unauthorized services or software are detected.

e. A violation of NASA policy is detected.

f. By approved written request from a Center, the OIG, OSPP, the General Counsel, or OHCM.

g. By court order.

16.1.4.3 Targeted monitoring when warranted and approved through the appropriate procedures may be performed by:

a. Center ITSMs.

b. Center IT security personnel and IT system administrators designated by the Center CIO.

c. NASA IT security personnel designated by the SAISO.

d. NASA law enforcement organizations as part of their investigation activities.

16.1.4.4 Targeted monitoring by NASA IT and IT security personnel in support of the NASA IT security program (i.e., resulting from anomalies found during routine monitoring or operation of NASA networks and services) is authorized under the service provider exception of the Electronic Communications Privacy Act.

16.1.4.5 Targeted monitoring by NASA IT and IT security personnel at the request of the NASA OIG, OSPP, or OHCM is performed on behalf of and under the authority of the requestor.

16.1.5 Approval for Targeted Monitoring by NASA IT and IT Security Personnel

16.1.5.1 Targeted monitoring is initiated after the Center ITSM or the NASA ITSO approves a request originating from a Center, the OHCM, the OIG, or the OSPP.

16.1.5.2 All requests for targeted monitoring will be formally submitted in writing.

16.1.5.3 All requests for targeted monitoring will be transmitted and stored according to NASA policies and guidelines, based on the sensitivity of the information contained therein.

16.1.6 Targeted Monitoring for Non-Criminal Matters

16.1.6.1 Requests shall include:

a. The requestor's name, title, and contact information.

b. Specification of the monitoring target (e.g., specific computer system).

c. Specific requirements for monitoring (e.g., monitor all incoming and outgoing activity).

d. Specific requirements for storage and handling of monitoring results.

16.1.6.2 A time limit, not to exceed three months, shall be set for monitoring requests.

16.1.6.3 After three months, a review and resubmission of the request are required to extend monitoring for another three months.

16.1.6.4 At the conclusion of the monitoring activity, the ITSM and/or monitoring

personnel will require a receipt acknowledging that official monitoring results were provided to the requestor.

16.1.7 Targeted Monitoring for Criminal or Counter-Intelligence Matters

16.1.7.1 Requests shall include:

a. The requestor's name, title, and contact information.

b. Official case number of the investigation being supported.

c. Specification of the monitoring target (e.g., specific computer system).

d. Specific requirements for monitoring (e.g., monitor all incoming and outgoing activity or monitor interactions from other entities across the network).

e. Specific requirements for storage and handling of monitoring results.

f. Authority under which monitoring is to be performed.

16.1.7.2 A time limit, not to exceed three months, shall be set for monitoring requests.

16.1.7.3 After three months, a review and resubmission of the request are required to extend monitoring for another three months.

16.1.7.4 At the conclusion of the monitoring activity, the ITSM and/or monitoring personnel will require a receipt acknowledging that official monitoring results were provided to the requestor.

16.1.8 Handling and Turning Over Evidence to Authorities

16.1.8.1 When performing requests for targeted monitoring on behalf of law enforcement officials such as the OIG or OSPP, monitoring personnel will be briefed by the requestor on their responsibilities and on the proper handling of monitoring results. Monitoring personnel may be asked to sign a non-disclosure agreement.

16.1.8.2 Whenever information containing results of routine or targeted monitoring activity is furnished, the ITSM and/or monitoring personnel will obtain a receipt from the official requestor. A record will be kept of all authorities and requesters receiving evidence.

16.1.9 Records Requirements

16.1.9.1 Information collected from routine and targeted monitoring shall be properly safeguarded and not released beyond the Center CIO, ITSM, and the monitoring personnel unless approved by the Center CIO and/or SAISO.

16.1.9.2 All releases of this data to a third party must be documented. Data collected during monitoring shall be stored by monitoring personnel in accordance with NASA records management policies. Law enforcement officers and other requesters will identify in their request any additional storage and handling requirements.

16.1.9.3 Law enforcement officials shall be responsible for storing and safeguarding data collected during targeted monitoring once this data has been furnished to them.

16.1.10 Research of New Monitoring Technology

16.1.10.1 To maintain an effective and current IT security capability, NASA may

occasionally develop or evaluate new monitoring tools or technology within the NASA environment. NASA will ensure that such testing, verification, and validation of monitoring technology not violate NASA policies and guidelines, nor endanger NASA resources and data.

16.1.10.2 In the course of testing, verifying, and validating monitoring technology within the NASA environment, only personnel authorized under this policy will install and run monitoring tools on NASA networks.

16.1.10.3 If external third party or contract technology is used, tested, validated, and verified using NASA resources (e.g., data, equipment, software, personnel, etc.) a testing agreement and protocol shall be in place and approved by the Center CIO or SAISO or designee.

16.1.10.4 All non-NASA or non-NASA-contractor personnel involved with the evaluation or development of monitoring technology shall sign a non-disclosure agreement.

16.1.11 Responsibilities

16.1.11.1 The NASA CIO shall maintain oversight of the NASA IT security monitoring program.

16.1.11.2 The SAISO:

a. Maintains responsibility and accountability for the NASA-wide implementation of the NASA IT security monitoring program.

b. Appoints, in writing, OCIO-sponsored NASA monitoring personnel with at least a U.S. secret clearance.

c. Informs the NASA CIO, as appropriate, about monitoring activity and findings.

d. Reviews and approves testing agreements and protocols for evaluations of monitoring technology in the NASA network environment.

16.1.11.3 The NASA ITSO:

a. Develops an appropriate use policy to be signed on a yearly basis by all monitoring personnel, which strictly forbids the sharing of all monitoring data without explicit permission from the appropriate NASA officials.

b. Reviews and approves requests for targeted monitoring from authorized NASA managers and law enforcement officials.

c. Informs NASA managers and the NASA SAISO as appropriate on the results of targeted monitoring.

16.1.11.4 The Center CIO:

a. Maintains responsibility and accountability for Center-specific implementation of the NASA IT security monitoring program.

b. Appoints, in writing, Center monitoring personnel with at least a U.S. secret clearance.

c. Informs the Center Director, as appropriate, of monitoring activity and findings.

d. Reviews and approves testing agreements and protocols for evaluations of monitoring

technology in the Center network environment.

16.1.11.5 The Center ITSM:

a. Reviews suspicious activities identified during routine monitoring to determine the course of action (e.g., whether activity appears criminal and warrants notification of law enforcement; whether non-criminal but suspicious activity warrants escalation to targeted monitoring and/or notification of other entities).

b. Notifies law enforcement of suspected criminal activities identified during monitoring.

c. Reviews and approves requests for targeted monitoring from authorized NASA managers and law enforcement officials.

d. Maintains documentation of all targeted monitoring activities involving the Center, including law enforcement or other requests for targeted monitoring and receipts for targeted monitoring records.

e. Ensures that all data collected from monitoring is properly safeguarded.

f. Informs NASA managers and the Center CIO as appropriate on the results of targeted monitoring.

g. Ensures that all monitoring personnel sign an appropriate use policy on a yearly basis, which strictly forbids the sharing of all monitoring data without explicit permission from appropriate NASA officials.

16.1.11.6 NASA and Center monitoring personnel:

a. Conduct monitoring as directed under the NASA IT security monitoring program.

b. Maintain audit logs of all routine monitoring activities, as well as identified suspicious activities recommended for further targeted monitoring.

c. Report to the Center ITSM or other appropriate management chain any suspicious activity identified during routine monitoring.

d. Provide technical support and monitoring services for approved targeted monitoring activities.

e. Inform the Center ITSM or NASA ITSO as appropriate on the progress and results of targeted monitoring.

f. Provide records of approved targeted monitoring to the requestor.

g. Properly safeguard all data collected from monitoring.

16.1.11.7 The NASA Deputy Inspector General shall review and validate all requests for targeted monitoring from the OIG to ensure they meet legal and administrative requirements.

16.1.11.8 The NASA Deputy Associate Administrator for Security and Program Protection shall review and validate all requests for targeted monitoring from the OSPP to ensure they meet legal and administrative requirements.

.

16.2 Periodic Testing and Security Controls Assessment

16.2.1 It is not feasible or cost-effective to monitor all of the security controls in an information system on a continuous basis. Therefore, each information system owner is required to use an appropriate subset of controls for periodic assessment and identify the frequency of such monitoring activity. The selection and frequency of testing are determined by the sensitivity and importance of the information system to NASA operations, NASA assets, or individuals.

16.2.2 Periodic Testing and Assessment of Security Controls Requirements

16.2.2.1 Information system owners shall conduct annual testing and assessment of the system security controls to assure effective controls.

16.2.2.2 Information system owners shall develop and maintain a prioritized list of security controls to be monitored, based on the results of the risk determination.

16.2.2.3 Information system owners shall maintain a list of security controls for periodic testing which contains the following information:

a. Priority, stated as one of the following levels as determined by the risk determination:

(1) High impact and high likelihood.

(2) High impact and moderate likelihood.

(3) Moderate impact and high likelihood.

(4) Moderate impact and moderate likelihood.

(5) High impact and low likelihood.

b. Security Control name.

c. Brief description of the control as it relates to the information system security level.

d. Brief description of the control objective.

e. Frequency of periodic assessment (i.e., quarterly, semiannual, annually).

16.2.2.4 The list of security controls to be monitored will be approved by:

a. System's AO and the NASA SAISO for the set of security controls for each master system plan.

b. System's AO and the Center CIO for the set of security controls for each subordinate system plan.

16.3 Continuous Monitoring Requirements

16.3.1 In addition to the continuous monitoring requirements in NIST SP 800-37, NASA systems shall:

a. Ensure that a self-assessment of each system is performed at least annually using the NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems, and ITS-SOP-0005-B, Procedure for Completing a NASA IT Security Program or System Assessment.

b. Ensure that an intrusion detection system (IDS) capability is implemented and

maintained to monitor traffic continually at the Network Security Perimeter (NSP) for security, performance, traffic analysis, and vulnerabilities.

c. Ensure that a full Center site survey is performed at least semiannually to detect unauthorized WLAN access points and to ensure that spot checks are performed quarterly.

16.4 Network Testing and Vulnerability Scanning

16.4.1 Despite the best efforts to include security measures and implement security controls in a system or application, there is no guarantee that these measures and controls will reliably prevent security incidents over time. Network testing and vulnerability scanning is one way to determine how well security measures and controls work at a particular point in time. The results of vulnerability scanning are very sensitive and, if not conducted under strict procedures, may affect the network or systems. Vulnerability scanning only determines the vulnerabilities that exist on a computer system without actually circumventing security processes and controls of the system being scanned.

16.4.2 NASA shall follow NIST SP 800-42, Guideline on Network Security Testing.

16.4.3 Network security testing and vulnerability scanning shall only be conducted with approval of the cognizant Center ITSM .

16.4.4 The NASA CIO shall issue directives for the scanning, elimination and mitigation, and reporting on specific high-risk vulnerabilities. The specific high-risk vulnerabilities shall be identified for scanning by the CCITS Manager in coordination with the Center ITSMs. The SAISO, CCITS Manager, and Center ITSM shall develop and maintain NASA ITS-SOP-0021, Vulnerability Scanning Procedures, on how vulnerabilities scanning is to be accomplished.

16.4.5 Results from network vulnerability scanning shall be marked and handled as ACI or SBU information.

16.5 Configuration Management

16.5.1 System security planned security controls need to be managed and maintained through configuration control processes. NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, provides additional information on the importance of configuration management. All NASA systems shall use the Agency's operating system and application configuration benchmarks.

16.5.1.1 IT security configuration management provides assurance that the system is the intended version (configuration) and that any changes to be made are reviewed for security implications. Configuration management can be used to help ensure that changes take place in an identifiable and controlled environment and that they do not unintentionally harm any of the system's properties, including its security. Changes to an information resource may present security implications because they may introduce or remove vulnerabilities and because significant changes may require updating the IT security plan or contingency plan, performing a risk analysis, and recertifying and accrediting the system.

16.5.1.2 The main security goal is to determine and document what changes occur, not

to prevent security from being changed. A second security goal of configuration management is to ensure that changes to the system are reflected in other documentation, such as the contingency plan. If the change is major, it will be necessary to reanalyze and document some or all of the system's security controls.

16.5.2 Hardware and Software Configuration Management Process Requirements

16.5.2.1 Hardware and software configuration management activities shall ensure that:

a. A configuration management policy and process that defines software and hardware standards for IT systems is developed and implemented.

b. A configuration management process is in place for each of their IT systems, including an approval and signoff process for changes to their IT systems (e.g., system enhancement, major changes to the software and hardware).

c. Standards are defined and maintained for IT systems.

d. Changes to a system do not diminish its security or functionality.

e. Current best practices for configuration management of major operating system types are published.

f. An effective patch management program is implemented and maintained that includes verification that patches have been properly applied to all systems.

g. An effective vulnerability reduction program to include periodic scanning for critical high-risk vulnerabilities is implemented and maintained.

16.5.3 Standard Operating System Process Requirements

16.5.3.1 The SAISO shall provide a mechanism to ensure that all IT resources comply with standard operating system benchmark templates. NASA will evaluate each system's operating system through a vendor-provided benchmarking capability.

a. All newly released benchmarks will be evaluated each year in October and May by the OCIO. Centers have four weeks to review benchmarks that are proposed for adoption.

b. To demonstrate compliance during reviews, Centers should ensure that their IT security plans document all deviations from the benchmarks. A complete list of available benchmarks will be made available by the vendor.

16.5.4 Network Configuration Control Board Requirements

16.5.4.1 The NCCB shall:

a. Ensure a level of risk relative to security and integrity of Center networked resources, which meets or exceeds Agency and Center requirements and expectations while maintaining an IT environment.

b. Be chaired by the Center CIO or designee.

c. Ensure that network security is addressed and will establish IP address management requirements.

d. Implement a secure process to adjudicate requests for access through the NSP for presentation to the NCCB.

e. Assign and manage all IP addresses including non-routable IP addresses behind firewalls or NAT boxes.

f. Maintain an up-to-date record of all NASA Integrated Services Network (NISN)-NISN-assigned IP addresses.

g. Monitor and document the Center's and Project's IP address ranges to ensure that Agency and Center policies have been addressed and any risk acceptance has been documented and authorized, as appropriate.

h. Ensure that security or vulnerability information on specific IP addresses is protected as ACI or SBU.

i. Have the authority to adjust bandwidth limits for traffic, including traffic between wireless access points and wired networks.

j. Report progress through the Center ITSM and SAISO.

k. Ensure the Center network is in compliance with Agency-networking standards.

l. Be subordinate to the Agency NSCB.

16.5.4.2 The Agency Network Security Control Board (NSCB)

16.5.4.2.1 The Agency NSCB shall:

a. Assure risk is mitigated to a level that maintains the security and integrity of Agency-networked resources, meets or exceeds Agency and Center requirements and expectations, and maintains a viable and secure IT environment.

b. Be chaired by the Deputy CIO for IT Security or his designee.

c. Have representation by each Center NCCB.

d. Ensure that network security is addressed at an Agency-level.

e. Implement a secure process to adjudicate requests for access through multiple Centers' NSPs or through the Agency NSP.

f. Report progress to the OCIO and CIO Board.

g. Recommend and review SOP technical standards and policies for implementation and operation of IT resources on NASA's networks.

h. Approve any change to the Agency Network Security Perimeter.

16.6 Additional Network and System Monitoring References

a. NPR 1441.1, NASA Records Retention Schedules.

b. NPD 1660.1, NASA Counterintelligence (CI) Policy.

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | Chapter12 | Chapter13 | Chapter14 | Chapter15 | Chapter16 | Chapter17 | Chapter18 | Chapter19 | Chapter20 | Chapter21 | AppendixA | AppendixB | ALL |

| NODIS Library | Legal Policies(2000s) | Search |

DISTRIBUTION:
NODIS